UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/782,825 | 02/14/2001 | Frank J. DiSanto | Copy-60 | 1728 |

7590 03/23/2005

Plevy & Howard
600 North Easton Road
Willow Grove, PA 19090

| EXAMINER | |
|---|---|
| CHAI, LONGBIT | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/782,825 | DISANTO ET AL. | |
| | Examiner | Art Unit | |
| | Longbit Chai | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/13/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1 – 28 have been presented for examination.

### *Response to Arguments*

1. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

2. Applicant's remarks Bjerrum teaches "to establish immediately a secure data or document transfer between two computer systems without having to exchange encryption / decryption keys between the computer systems" is a teach away from "determining a next encryption key". Examiner notes Bjerrum teaches, instead of exchange encryption / decryption keys directly between the computer systems, the system derive the next encryption key based on a previously exchanged random number (i.e. retained encryption key) (Bjerrum: see for example, Column 37 Line 52 – 56) so that the security can be enhanced by ensuring the secured communications between any two stations without having to exchange encryption / decryption keys directly between the computer systems.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1 – 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro (Patent Number: 6009176), hereinafter referred to as Gennaro, in view of Bjerrum (Patent Number: Re.36310), hereinafter referred to as Bjerrum.

3. As per claim 1, 11 and 20, Gennaro teaches a method for securely exchanging information items used to generate encryption keys among at least two parties using a public/private encryption key system over a communication network, each of said parties retaining an initial private key and transmitting an initial corresponding information item used by each receiving party to determine, and retain, an initial encryption key, said method comprising the steps of:

a. determining a next private key and a next corresponding information item set, wherein said next private key is retained among said retained next private keys (Gennaro: see for example, Column 7 Line 12 – 15 and Column 7 Line 19 – 24: Gennaro teaches the previous private key SK (i – 1) needs to be retained in order to decrypt the current data block (i));

4. Gennaro teaches determining a next encryption key from said next private key, wherein said next encryption key is retained among said retained encryption keys (Gennaro: see for example, Column 7 Line 12).

5. Gennaro does not teach expressly determining a next encryption key from said next private key and said received information item, wherein said next encryption key is retained among said retained encryption keys.

6. Bjerrum teaches determining a next encryption key from said received information item, wherein said next encryption key is retained among said retained encryption keys (Bjerrum: see for example, Column 37 Line 52 – 56: Bjerrum teaches encryption key is made by use of a previously exchanged random number).

7. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bjerrum within the system of Gennaro because (a) Gennaro teaches encryption / decryption of the security sensitive information based on previously retained encryption / decryption keys and (b) Bjerrum discloses encryption / decryption of the security sensitive information can be further based on previously exchanged random number to enhance the security to ensure the secured communications between any two stations.

8. Therefore, Gennaro as modified further teaches:

b. determining a next encryption key from said next private key and said received information item, wherein said next encryption key is retained among said retained encryption keys (Gennaro: see for example, Column 7 Line 12) & (Bjerrum: see for example, Column 37 Line 52 – 56).

c. encrypting at least one element of said next information item using an encryption key selected from said retained encryption keys (Bjerrum: see for example, Column 37 Line 12 – 13);

d. transmitting said next information item over said network (Bjerrum: see for example, Column 3 Line 1 – 2);

e. decrypting a received encrypted information item element using a private key selected from said retained private keys (Bjerrum: see for example, Column 37 Line 17 – 20) & (Gennaro: see for example, Column 7 Line 12).

9. As per claim 2, Gennaro as modified teaches the claimed invention as described above (see claim 1). Gennaro as modified further teaches steps a-e are repeated until a known number of encryption keys are determined (Gennaro: see for example, Column 3 Line 25 – 26, Column 5 Line 44 – 46, Column 7 Line 12 – 15 and Column 7 Line 19 – 24: Gennaro discloses a known number of encryption keys need to be determined in order to repeat for all the data blocks in a digital stream which is being divided into a known number of data blocks because the previous private key SK (i – 1) needs to be retained in order to decrypt the current data block (i)).

10. As per claim 3, 12 and 21, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches said information item element is a public key (Bjerrum: see for example, Column 18 Line 59 – 60: Bjerrum teaches the encryption key can be created based on other person's public key as well as his own digital signature (i.e. his own private key).

11. As per claim 4, 13 and 22, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches said information item element is a synchronizing indicator (Bjerrum: see for example, Column 37 Line 52 – 56: Bjerrum teaches encryption key is made by use of a previously exchanged random number which is qualified as a synchronizing indicator).

12. As per claim 5, 14 and 23, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches selecting at least one of said retained encryption keys alternatively (Bjerrum: see for example, Column 22 Line 45 – 47: Bjerrum teaches data encryption keys being used were arranged in a known sequence (or pre-selected order) beforehand. One of ordinary skill in the art, furthermore, would have expected choosing the encryption alternatively as one form of a pre-selected orders can perform equally well with other options because either selection performs the same function of preventing security bleaching).

13. As per claim 6, 15 and 24, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches selecting a known encryption key (Bjerrum: see for example, Column 22 Line 45 – 47: Bjerrum teaches data encryption keys being used were arranged in a known sequence (or pre-selected order) beforehand).

14. As per claim 7, 16 and 25, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches known encryption key is such that an output value is the same as an input

value (It is evident that no encryption s needed as long as the communication is secured).

15. As per claim 8, 17, 18 and 26, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches encryption keys are selected in a known sequence (Bjerrum: see for example, Column 22 Line 45 – 47: Bjerrum teaches data encryption keys being used were arranged in a known sequence (or pre-selected order) beforehand).

16. As per claim 9, 19 and 27, Gennaro as modified teaches the claimed invention as described above (see claim 1, 11 and 20 respectively). Gennaro as modified further teaches known sequence corresponds to an order of retention of said encryption keys (Bjerrum: see for example, Column 37 Line 12 – 13 and 22 Line 45 – 47).

17. As per claim 10 and 28, Gennaro as modified teaches the claimed invention as described above (see claim 1 and 20 respectively). Gennaro as modified further teaches known sequence corresponds to an order pre-selected by said parties (Bjerrum: see for example, Column 22 Line 45 – 47: Bjerrum teaches data encryption keys being used were arranged in a known sequence (or pre-selected order) beforehand).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100